STEPTOE & JOHNSON

DOCKET FILE COPY ORIGINAL

ATTORNEYS AT LAW

1330 CONNECTICUT AVENUE, N.W.
WASHINGTON, D.C. 20036-1795

(202) 429-3000
FACSIMILE: (202) 429-3902
TELEX: 89-2503

PHOENIX, ARIZONA
TWO RENAISSANCE SQUARE

TELEPHONE: (602) 257-5200
FACSIMILE: (602) 257-5299

STEPTOE & JOHNSON INTERNATIONAL
AFFILIATE IN MOSCOW, RUSSIA

TELEPHONE: (011-7-501) 258-5250
FACSIMILE: (011-7-501) 258-5251

STEWART A. BAKER
(202) 429-6413
sbaker@steptoe.com

May 20, 1998

Via HAND DELIVERY

Ms. Magalie Roman Salas
Secretary
Federal Communications Commission
Room 222
1919 M Street, N.W.
Washington, D.C. 20554

RE: CC Docket No. 97-213:
Comments of The Telecommunications Industry Association

Dear Ms. Salas:

On behalf of The Telecommunications Industry Association, enclosed for filing are an original and four (4) copies of Comments of The Telecommunications Industry Association in the above-referenced proceeding.

Also enclosed is an additional copy that we ask you to date-stamp and return with our messenger.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Stewart A. Baker

Counsel for
Telecommunications Industry Association

Enclosures

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of: **Communications Assistance for Law Enforcement Act** **Petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by Center for Democracy and Technology** **Joint Petition for Expedited Rulemaking, filed by Federal Bureau of Investigation and U.S. Department of Justice** **Petition for Rulemaking, filed by Telecommunications Industry Association**	**CC Docket No. 97-213**

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

Stewart A. Baker
Thomas M. Barba
Maury D. Shenk
Steptoe & Johnson LLP
1330 Connecticut Ave., N.W.
Washington, D.C. 20036
(202) 429-3000

Counsel for Telecommunications Industry Association

Matthew J. Flanigan
President
Grant Seiffert
Director of Government Relations
Telecommunications Industry Association
1201 Pennsylvania Ave., N.W.
Suite 315
Washington, D.C. 20004
(202) 783-1338

May 20, 1998

SUMMARY

In 1994, after a long lobbying campaign by the Federal Bureau of Investigation ("FBI"), Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA") to address the FBI's concerns.

But CALEA was not exactly the law that the FBI had asked for. It was a compromise. Now, four years later, the FBI's Joint Petition with the Department of Justice ("DOJ") essentially asks the Commission to undo the careful legislative compromise and give the FBI what it was unable to obtain from Congress.

The DOJ and FBI position is quite frankly breathtaking in its disregard for what the law says. First, DOJ and FBI ask the Commission to adopt a test that cannot be found in CALEA. Then, they ask the Commission to declare the test satisfied on the basis of evidence that cannot be found in the record. The test advanced by the DOJ and FBI is that carriers must supply law enforcement with those features and data that have "always been available" in past law enforcement wiretaps. Yet, they provide almost no empirical evidence to support their claims that this data has, in fact, "always" been available in response to wiretap orders. The lack of evidence on the record is particularly telling because only one party to these proceedings has access to such information. Almost all of the data with respect to wiretap practice over the past 30 years is locked in the case files of DOJ and FBI.

But lack of a proper record is only one of many reasons to reject the DOJ/FBI approach. If the Commission were to adopt a "historically available" test as the touchstone for what CALEA requires, arguments over its scope would never end. At

what time in history is availability to be measured? In what part of the country? Using what equipment? At what cost? The FBI and DOJ do not say.

Perhaps more remarkable still, even historic availability – their own standard – is not enough to support many of the features that DOJ and FBI demand, as they candidly recognize at several points. If the law enforcement position were to prevail, telecommunications manufacturers would be required to design new equipment based not just on what was once available to law enforcement but also on such vague notions as the "convenience" of law enforcement or law enforcement "preferences" for particular implementations.

The Commission should resist the invitation of DOJ and FBI to stray from the careful balance and clear language of CALEA. Section 103 of CALEA sets forth a carefully prioritized and clear set of rules for providing law enforcement access to the many different kinds of information that are generated by a telecommunications carrier.

Most important to law enforcement is access to the contents of criminal suspects' communications. CALEA assigns access to such contents the highest priority. Carriers and their equipment must provide law enforcement with expeditious access to the contents of a call. But only one of the FBI's allegations of deficiency falls into this area – i.e., the remarkable claim that telecommunications carriers must deliver the content of conference calls even though no person subject to a wiretap order is participating. This claim clearly fails because CALEA covers only calls "to or from" the intercept subject's facilities, and because the statutory and constitutional authority for wiretaps does not extend as far as DOJ and FBI contend.

CALEA's second priority is the provision of "call-identifying information." But unlike call content, the obligations of carriers and their equipment are more limited. First, they must provide call-identifying information only if it is "reasonably available" to the carrier. This limitation is consistent with the long-standing judicial principle that parties providing assistance to law enforcement cannot be asked to undertake unreasonable burdens. Second, this category of information is narrowly defined – i.e., which phone number the parties are calling from, which they are calling to, whether the call is redirected, and the like.

The DOJ/FBI Petition alleges three "deficiencies" of J-STD-025 with respect to information that it claims to be call identifying information – subject-initiated dialing and signaling information, party hold/party join/party drop messages, and network-generated signaling information. The petition also asserts two related "deficiencies": the expeditious delivery of call-identifying information and the delivery of all call-identifying information on the "call data channel." Most of these claims fail for one of two simple reasons: either the requested capability is already provided by J-STD-025 or, more importantly, it is not reasonably available to carriers. The effort of DOJ and FBI to force capabilities that are not reasonably available into the industry standard shows that the capabilities would not be available in the absence of a change in the telecommunications network design. When Congress said that information should be provided to the FBI if it is reasonably available to the carrier, Congress did not mean "reasonably available once the FBI is through designing the network." In a few instances the DOJ and FBI requests fail because not even the DOJ and FBI can

find a statutory basis for their claims; they candidly admit, for example, that CALEA does not support their "call data channel" request.

The lowest priority set by Congress is for all the other information that may be available about telephone calls and telephone networks but that is not call content or call-identifying information. Simply put, this data is not covered by CALEA. Congress imposed no special obligation to gather or supply this information. That is not to say that the information will be denied to law enforcement. Quite the contrary, where information is available in the hands of a telephone carrier, it may be subpoenaed by law enforcement. Its absence from CALEA simply means that there is no obligation for industry standards to do something special to deliver the information to the government in an expeditious basis.

Despite the fact that CALEA is quite clear on this point, DOJ and FBI allege that J-STD-025 is "deficient" for failure to provide four capabilities in this category: three types of surveillance status information and standardization of interface protocols. These requests lack any support in the text of CALEA.

Finally, in addition to prioritizing the data to be supplied to law enforcement, CALEA sets a very different priority for the way that data is be intercepted and delivered to law enforcement. This must be accomplished in a manner that protects the privacy of the communications. The Center for Democracy and Technology claims that J-STD-025 is "deficient" for failure to meet this obligation with respect to location tracking information and packet data. TIA submits that the standard is fully consistent with CALEA in these two areas as well.

The wiretap assistance rules established by CALEA are entirely reasonable. But they do not do what the FBI wanted CALEA to do – provide full control over future telecommunications design combined with "one-stop-shopping" convenience for wiretaps. It is remarkable that four years after the statute became law, DOJ and FBI have essentially urged this Commission to throw out the statute Congress wrote and substitute in its place a formless and open-ended set of obligations that will produce unending litigation and uncertainty. The Commission should reject this invitation and find that J-STD-025 is a valid industry standard.

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of: **Communications Assistance for Law Enforcement Act** **Petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by Center for Democracy and Technology** **Joint Petition for Expedited Rulemaking, filed by Federal Bureau of Investigation and U.S. Department of Justice** **Petition for Rulemaking, filed by Telecommunications Industry Association**	**CC Docket No. 97-213**

To: The Commission

COMMENTS OF THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION

The Telecommunications Industry Association ("TIA") submits these comments pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act ("CALEA"),[1] Sections 1.415 and 1.419 of the Commission's Rules,[2] and

[1] 47 U.S.C. § 1006(b). CALEA was adopted as Pub. L. No. 103-414, 108 Stat. 4279 (1994).

[2] 47 C.F.R. §§ 1.415, 1.419.

the Commission's April 20, 1998 Public Notice,[3] to respond to the Joint Petition for Expedited Rulemaking, filed by Federal Bureau of Investigation and U.S. Department of Justice on March 27, 1998 (the "DOJ/FBI Petition") and the Petition for Rulemaking under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act, filed by Center for Democracy and Technology on March 26, 1998 (the "CDT Petition"). In addition, these comments address issues raised in the Petition for Rulemaking filed by TIA on April 2, 1998 (the "TIA Petition").[4]

The DOJ/FBI Petition and the CDT Petition challenge the industry "safe harbor" standard J-STD-025[5] (which is a valid interim industry standard approved by TIA and Accredited Standards Committee T1, and published on December 8, 1997 pursuant to

---

[3] Public Notice, DA 98-762 (Apr. 20, 1998).

[4] In separate comments filed on May 8, 1998 and May 15, 1998, TIA has responded to the Commission's request for comments on extension of the CALEA compliance date. See Comments of the Telecommunications Industry Association (May 8, 1998) ("TIA Extension Comments"); Reply Comments of the Telecommunications Industry Association (May 15, 1998) ("TIA Extension Reply Comments").

[5] Telecommunications Industry Association, J-STD-025, Interim Standard (Trial Use Standard): Lawfully Authorized Electronic Surveillance (Dec. 8, 1997) ("J-STD-025"). TIA has provided complementary copies of this copyrighted document to the Commission staff for their use in this and related proceedings. The cover page and table of contents of J-STD-025 are attached as an exhibit to the DOJ/FBI Petition. TIA requests that the Commission respect the intellectual property rights of TIA and the Alliance for Telecommunications Industry Solutions in this copyrighted document. See, e.g., 47 C.F.R. §§ 1.1307(b)(4) & 68.317 (using copyrighted American National Standards Institute ("ANSI") standards without disclosing their contents); see also Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities, 63 Fed. Reg. 8545, ¶ 6j (Feb. 19, 1998) (specifying that an agency "should reference voluntary consensus standards, along with sources of availability, in appropriate publications, regulatory orders, and related internal documents . . . . If a voluntary standard is used and published in an agency document, [the Commission] must observe and protect the rights of the copyright holder and any similar obligations.").

Section 107(a)(2) of CALEA[6]) under Section 107(b) of CALEA, and argue that the Commission should adopt rules providing standards for CALEA compliance that are different from those in J-STD-025.

The nearly simultaneous filing of the DOJ/FBI Petition and the CDT Petition highlights the dilemma that the telecommunications industry has faced in CALEA negotiations for a period of more than three years. Law enforcement and privacy groups have advanced alternative views of the scope of the statute, while industry has sought to reach a good faith compromise that adopts an interpretation of CALEA that is supported by the statute and legislative history. TIA submits that J-STD-025 represents such an approach, and accordingly requests that the Commission deny both the DOJ/FBI Petition and the CDT Petition.

The determinative legal issue in this proceeding is whether J-STD-025 satisfies the assistance capability requirements of Section 103(a) of CALEA.[7] Under Section 107(b) of CALEA, the Commission's inquiry is limited to determining whether, based upon an analysis of specific statutory factors, J-STD-025 is "deficient" for failure to satisfy the requirements of Section 103(a). The Commission must reject the efforts of DOJ and FBI to impose intercept capability requirements on the telecommunications industry on bases that are not supported by Section 103(a) (or any other provision of CALEA). For reasons set out in detail below, TIA respectfully requests the Commission to deny both the

[6] 47 U.S.C. § 1006(a)(2).

[7] 47 U.S.C. § 1002(a).

DOJ/FBI Petition and the CDT Petition, and to recognize J-STD-025 as a valid industry standard that is consistent with CALEA.

BACKGROUND

A. CALEA

Congress enacted the Communications Assistance for Law Enforcement Act in 1994 in order to "preserve the government's ability . . . to intercept communications involving advanced technologies . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services.[8] CALEA did not replace the basic statutory framework for authorization of wiretaps – which is contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[9] as amended by the Electronic Communications Privacy Act of 1986 ("ECPA").[10] Rather, the purpose of CALEA was "to further define the industry duty to cooperate [with wiretaps] and to establish procedures based on public accountability and industry standards-setting."[11]

Congress made it very clear in enacting CALEA that the statute was not driven by just one purpose, but involved a balancing of competing interests. In defining telecommunications industry duties under CALEA, Congress weighed the asserted needs

---

[8] H.R. Rep. No. 103-827, Pt. 1, at 9 (1994) ("CALEA House Report").

[9] Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2511-2521 & 3121-3127). A court order under Title III requires a telecommunications carrier to "furnish . . . all information, facilities, and technical assistance necessary to accomplish the interception . . . ." 18 U.S.C. § 2518(4).

[10] Pub. L. No. 99-508, 100 Stat. 1848 (1986)

[11] CALEA House Report at 14.

of law enforcement against the interests of privacy, innovation and efficiency. Accordingly, Congress sought

> to balance three key policies: (1) to preserve a **narrowly focused** capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies.[12]

In interpreting CALEA, the Commission must be careful to balance the competing policies considered by Congress, rather than to focus only on satisfaction of the needs of law enforcement, as DOJ and FBI urge. The "hallmark" of CALEA, as FBI Director Freeh has testified, "is reasonableness."[13]

Another important, and unusual, aspect of CALEA is that there is no agency responsible for overall implementation of the statute. While the Commission plays certain important roles in implementation of CALEA, it is the telecommunications industry, in the first instance, that is responsible for adopting standards for design of networks that comply with the statute. Under CALEA, with regard to network design, "[i]ndustry, not a government official, runs the show."[14]

---

[12] Id. at 13 (emphasis added).

[13] Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong. 115 (March 18 & Aug. 11, 1994) ("Joint Hearings") (prepared statement of Louis J. Freeh on behalf of the Federal Bureau of Investigation).

[14] Joint Hearings at 111 (prepared statement of Sen. Patrick J. Leahy).

CALEA explicitly restricts the role of law enforcement in design of CALEA-compliant networks.[15] Law enforcement agencies are not authorized "to require the adoption of any specific design of equipment, facilities, services, features, or system configurations" or "to prohibit the adoption of any equipment, facility, service, or feature" by any telecommunications carrier or equipment manufacturer.[16] Recently, Senator Leahy, one of the original sponsors of CALEA, stated: "This law did not give a license to the FBI to redesign our telecommunications networks to suit its purposes."[17] Indeed, FBI Director Freeh himself has stated that "law enforcement has no intention of becoming a technology czar or of regulating the development of new and beneficial telecommunications systems, services or features."[18]

The provisions of CALEA at issue in this rulemaking proceeding – Sections 103 and 107 of the statute – make clear the general limitations on CALEA obligations imposed by Congress and the primary role of the telecommunications industry in

---

[15] Those who were involved in the drafting of CALEA may recall that the original first draft circulated by the FBI had the Commission creating compliance standards, had ratepayers paying all costs, and placed an embargo on any new additions to the network until all switches met the proposed requirements. Due to industry and consumer uproar, this was quickly replaced with a draft that vested full power for the standard and control in DOJ. This was also soundly rejected, and the final language that passed as CALEA clearly has a balanced approach that effectively eliminates law enforcement control over the network design process.

[16] 47 U.S.C. § 1002(b)(1); see also CALEA House Report at 19 (CALEA "expressly provides that law enforcement may not dictate system design features and bar introduction of new features and technologies.").

[17] Sen. Leahy Statement on Implementation of CALEA Act, U.S. Newswire (Mar. 27, 1998).

[18] Joint Hearings at 115-16 (prepared statement of Louis J. Freeh on Behalf of the Federal Bureau of Investigation).

implementation of CALEA. These provisions also carefully define the nature of the Commission's review, in a proceeding like the present one, of industry standards like J-STD-025 that are adopted for CALEA compliance.

The affirmative obligations of CALEA at issue in this proceeding are the "assistance capability requirements" of Section 103 of CALEA.[19] Under Section 103(a), telecommunications carriers must, to the extent "reasonably achievable,"[20] have the capability (1) to deliver the content of communications to law enforcement, (2) to deliver "reasonably available" call-identifying information to law enforcement, (3) to make such information available to law enforcement at remote locations, and (4) to protect the privacy of intercepted communications and the security of information regarding the interceptions.[21] It is these requirements that J-STD-025 implements, and it is these requirements that are the basis of the DOJ/FBI Petition and the CDT Petition.

---

[19] 47 U.S.C. § 1002. The other principal category of CALEA obligations are the capacity requirements of Section 104, 47 U.S.C. § 1003, which are not at issue in this proceeding. Under Section 104, DOJ was required to establish, in consultation with the telecommunications industry and standards-setting organizations, maximum interception capacity requirements, with which the telecommunications industry will be required to comply. Although the deadline for establishment of such capacity requirements was October 25, 1995, DOJ did not issue its final capacity notice until March 12, 1998, more than two years late. See Federal Bureau of Investigation, Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 63 Fed. Reg. 12,218, 12,200 (Mar. 12, 1998).

[20] See 47 U.S.C. §§ 1002(a), 1008(b). DOJ is authorized to pay reasonable costs directly associated with achieving compliance with the assistance capability requirements for equipment installed or deployed after January 1, 1995, if such compliance would otherwise not be "reasonably achievable." See id. § 1008(b).

[21] See 47 U.S.C. § 1002(a). The October 25, 1998 statutory deadline for compliance with these obligations may be extended by the Commission. See 47 U.S.C. §§ 1006(c), 1009. The extension of this compliance date is the subject of numerous separate comments filed in this rulemaking proceeding.

Congress explicitly cautioned against "overbroad interpretation" of the assistance capability requirements of Section 103.[22] "[C]arriers are required to comply [with assistance capability requirements] only with respect to services or facilities that provide a customer or subscriber with the ability to originate, terminate or direct communications."[23] Furthermore, a carrier need only assist interception of communications which are in its control, a question which "will depend on the design of the service or feature at issue . . . ."[24] In addition, if call-identifying information "is not reasonably available, the carrier does not have to modify its system to make it available."[25]

Section 107 of CALEA[26] provides the Commission's authority to consider the DOJ/FBI Petition and the CDT Petition. Section 107(a) contains a "safe harbor," providing that telecommunications carriers and equipment manufacturers are considered to be in compliance with the assistance capability requirements of Section 103 if they comply with "publicly available technical requirements or standards adopted by an industry association or standard-setting organization . . . to meet the requirements of section 103."[27] Section

---

[22] CALEA House Report at 22. See also id. at 17 ("[A]s the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and properly limited") (emphasis added) & 23 ("The Committee expects industry, law enforcement and the FCC to narrowly interpret the requirements.") (emphasis added).

[23] Id. at 18.

[24] Id. at 22.

[25] Id.; see also 47 U.S.C. § 1002(a)(2).

[26] 47 U.S.C. § 1006.

[27] 47 U.S.C. § 1006(a)(2).

107(a) thus provides that telecommunications industry organizations, in the first instance, are responsible for setting standards that satisfy the requirements of Section 103 of CALEA.[28]

Section 107(b) of CALEA gives the Commission authority to resolve disputes that arise where a government agency or other person believes that industry-adopted standards are "deficient." In considering such disputes, the Commission is required to evaluate factors relating to (1) cost-effectiveness, (2) protecting privacy and security of communications, (3) minimization of costs to ratepayers, and (4) encouraging provision of new technologies and services to the public.[29] Thus, Section 107(b) explicitly indicates that the Commission's review of J-STD-025 must be based upon consideration of the various competing interests that Congress considered in adopting CALEA.

In sum, CALEA is a carefully-conceived statute that seeks to preserve a reasonably-focused ability of law enforcement to intercept the content of wire and electronic communications, as well as reasonably available associated call-identifying information, while not impairing the important interests of the public in privacy, reasonable telecommunications rates, and innovation. In considering the DOJ/FBI Petition and the CDT Petition, the Commission should carefully consider these statutory policies, as well as the defined standards of review imposed on the Commission by Sections 103 and 107 of CALEA.

---

[28] See CALEA House Report at 26-27 (discussing delegation of authority to set standards).

[29] See 47 U.S.C. § 1006(b); see also CALEA House Report, at 27.

B. Implementation of CALEA

As the Commission is aware, in November 1994 TIA began organizing a standards process to implement CALEA's assistance capability requirements almost immediately after the passage of the CALEA.[30] TIA's efforts were initially limited to developing a standard for the wireless telephony industry; it was assumed that Committee T1, sponsored by the Alliance for Telecommunications Industry Solutions ("ATIS"), would develop a standard for the wireline industry. Eventually, TIA and Committee T1 decided to combine their efforts and establish a joint standard for the wireline and wireless industries, with TIA taking the lead role.

TIA's Engineering Committee TR 45 met with the FBI in late 1994 to begin to understand the views of law enforcement on CALEA implementation. In May 1995, TIA formally initiated a CALEA standards program – Project Number ("PN") 3580 – under the auspices of TIA Subcommittee TR 45.2. TR 45.2 determined to complete a CALEA standard on an expedited basis. Working with the FBI – which attended almost every standards meeting – TR 45.2 completed an initial draft standard by October 1995.

At the FBI's request, however, this early draft was not finalized or put to a ballot, in order to give the FBI an opportunity to prepare its Electronic Surveillance Interface ("ESI") document and make technical contributions to the standard. Through the spring of 1996, the FBI asked that industry delay its work until the FBI could complete and distribute its ESI document. Beginning in May, draft portions of the ESI were leaked to

---

[30] See TIA Extension Comments at 14-18.

certain members of TR 45.2 but, because the document had not been publicly released, the FBI asked that the document not be discussed. Finally, at the July 11, 1996 meeting of TR 45.2, the final draft of the ESI (dated June 24, 1996) was released to the subcommittee.[31]

The ESI was considerably more expansive than TIA's draft standard. Although the industry believed that many of the requirements in the FBI's ESI were not mandated by CALEA, the industry sought to reach a consensus standard with the FBI and reconcile their differences. Beginning in September 1996, a series of "legal summits," conducted under the auspices of the Cellular Telecommunications Industry Association ("CTIA"), were held to resolve legal disputes relating to the FBI's asserted requirements. In addition, TR 45.2 continued to seek a compromise with law enforcement, adding several features in an attempt to satisfy law enforcement's requirements.

After several months of extended negotiations, however, TR 45.2 recognized that compromise was not going to be possible. The FBI continued to insist on a handful of features that were not provided for in the industry standard – which became known as the "punch list."[32] The FBI provided several reasons for why it needed these features – such

---

[31] The ESI is attached to the DOJ/FBI Petition.

[32] A February 12, 1997 version of the "punch list" (the "February 1997 Punch List") is attached as Exhibit 1. The term "punch list" is generally used in the construction industry to refer to a list of relatively minor items that are required to be completed under a construction contract. While the FBI may have chosen this term to suggest that an analogous situation exists with respect to the CALEA standards process, the situation is in fact very different. The FBI punch list consists of items that not required to be provided under CALEA, that are not minor, and that would impose substantial burdens on telecommunications carriers.

as "core evidentiary/'minimization'," "integrity of interception efforts," and "manageability of effecting interception"[33] – none of which are mentioned under CALEA.

In March 1997 the subcommittee submitted its standard – Standards Proposal ("SP")-3580 – to an ANSI public inquiry ballot. As TIA has explained in its comments on extension of the deadline for CALEA compliance, the FBI decided to prevent industry's adoption of its own standard.[34]

After the defeat of SP-3580, TR 45.2 revised the standard in response to comments from law enforcement and others (including privacy groups like CDT), and submitted the revised standard, SP-3580A, to an ANSI vote in the summer of 1997. Simultaneously, the subcommittee also balloted the standard as an industry interim/trial use standard, on which only industry participants were entitled to vote.[35] Again, the FBI objected that the revised standard failed to include several punch list items,[36] and the proposed ANSI standard failed to achieve consensus – despite almost unanimous approval by industry participants – because of an enormous number of "no" votes

---

[33] See February 1997 Punch List.

[34] TIA Extension Comments at 16-17.

[35] Ironically, FBI participants in the standards process had originally urged TR 45.2 to ballot its standard as an interim/trial use standard. They expressed concern that an ANSI ballot would be in the public domain and indicated that they would prefer the industry standard to be a proprietary TIA document. TR-45.2, noting that CALEA permitted "any person" to challenge the standard under Section 107, decided that an ANSI public inquiry ballot might be the more appropriate method of balloting since this would actively solicit input from other interested parties, such a privacy groups. Privacy advocates did, in fact, return ballots on the standard.

[36] An August 11, 1997 presentation on the "missing capabilities" is attached as Exhibit 2.

submitted by law enforcement agencies that had not directly participated in the standards process. The industry interim standard, however, was approved by TR 45.2 for submission for publication as an interim/trial use standard.

On December 5, 1997, TIA and Committee T1 jointly published the interim/ trial use industry standard as J-STD-025, the standard at issue in this proceeding. The FBI immediately denounced the standard as deficient because it did not include the punch list items. Contemporaneously, on December 3, 1997, in a continued effort to seek a possible compromise with the FBI, TIA conducted an all-day engineering summit to review the technical feasibility of the FBI's eleven punch list features. The meeting was held, in part, because of FBI belief that industry was misinterpreting the punch list requirements and that it might be possible to clarify these requests in such a way as to reduce the technical difficulty of providing the punch list features. During the meeting, engineers from both the telecommunications industry and the FBI closely analyzed each of the punch list features.[37]

Also at approximately the same time, the FBI advised the telecommunications industry that it had initiated a legal review of the punch list features by the Department of Justice's Office of Legal Counsel. The FBI advised that it would share the result of this legal analysis with industry once it was completed. Although the analysis

[37] The memorandum and overhead slides prepared during the meeting to summarize this discussion are attached as Exhibit 3. See FBI Clarifications/Comments on "Punchlist" Features, at 2 (Dec. 3, 1997) ("FBI December 1997 Clarifications").

has never been provided to industry, it was summarized in a February 3, 1998 letter from Assistant Attorney General Steve Colgate.[38]

While the Colgate Letter stated that DOJ and FBI had concluded that two of the items on the punch list were not required by CALEA,[39] both of these features were incorporated in a document subsequently submitted by the FBI during the March 10 & 11, 1998 Enhanced Surveillance Services ("ESS") standards meeting in Austin, Texas.[40] This again demonstrates that even when the DOJ has agreed with industry that an item on the punch list is not required by CALEA, the FBI disregards that conclusion and continues to argue for and request the feature. In addition, the FBI also requested a timing requirement that the FBI had modified during the December engineering summit. In a subsequent letter to the major telecommunications associations, Attorney General Janet Reno sought to clarify the confusion created by the FBI's submission.[41] Nevertheless, one of the features identified by DOJ as exceeding the scope of CALEA (standardization of interface protocols) has reappeared as a requested capability in the DOJ/FBI Petition.[42]

---

[38] See Letter from Stephen R. Colgate, Assistant Attorney General, to Tom Barba, Steptoe & Johnson LLP (Feb. 3, 1998) ("Colgate Letter") (attached as Exhibit 4).

[39] See id. at 3.

[40] TR 45.2 initiated the ESS process in February 1998, at the request of CTIA, to standardize the FBI's punch list requirements in the event that such items were ever determined to be required by CALEA.

[41] Letter from the Honorable Janet Reno, Attorney General, to CTIA, Personal Communications Industry Association ("PCIA"), TIA and United States Telephone Association ("USTA") (March 18, 1998) (attached as Exhibit 5).

[42] See DOJ/FBI Petition at 57-58.

The validity of J-STD-025 and the issues raised in the FBI punch list are now before the Commission in this proceeding – as a result of the filing of the CDT Petition on March 26, 1998 and the DOJ/FBI Petition on March 27, 1998.

C. J-STD-025

J-STD-025 is a 150-page technical document setting out standards for CALEA compliance by providers of wireline and wireless telephony services.[43] Most of the technical aspects of J-STD-025 are not in dispute in this proceeding, and those technical issues which are in dispute are addressed below in the context of the specific challenges raised by DOJ, FBI and CDT. Nevertheless, a brief description of the structure of J-STD-025 is useful to inform this discussion.

Sections 1-3 of J-STD-025 provide background information: an introduction, a list of references, and a glossary of definitions and acronyms. Section 4 of the standard describes the basic structure of interceptions pursuant to Title III and CALEA, including the various roles of carriers and law enforcement in the interception process, and the provision of various types of intercept-related information over call content channels ("CCCs") and call data channels ("CDCs"). In addition, Section 4 provides pictorial descriptions of the

[43] As the Department and FBI note in their joint petition, J-STD-025 only applies to the wireline, cellular and broadband PCS carriers on which the FBI has focused its attention. See DOJ/FBI Petition at 4. See also Federal Bureau of Investigation, Implementation of Section 104 of the Communications Assistance for Law Enforcement Act, 63 Fed. Reg. 12218, 12220 (March 12, 1998). The standard does not establish CALEA capability requirements for several industries (e.g., paging and satellite) that the FBI has asserted are covered by CALEA.

basic interfaces between telecommunications carriers and law enforcement for the various types of communications covered by J-STD-025.

Section 5 of J-STD-025 describes the specific information that is provided for an interception, including both call content and call-identifying information. The section describes a series of messages for conveying call-identifying information to law enforcement (e.g., the TerminationAttempt message is generated when an intercept subject receives an incoming call), and defines the parameters that are provided in each such message. Section 6 of the standard establishes requirements for the communications protocols that are used in the interface between telecommunications carriers and law enforcement. The section also uses the generic Abstract Syntax Notation One ("ASN.1") developed by the International Telecommunication Union to explain how the messages defined in section 5 are transmitted to law enforcement via the protocols described in section 6.

The annexes to J-STD-025 (which do not technically form a part of the standard) provide a substantial amount of additional information. Annexes A through D provide detailed examples of the implementation of J-STD-025 in various situations and for various types of communications. Of particular interest, Annex D describes the call data messages that J-STD-025 requires to be generated for particular types of calls. Annex E describes an additional, optional data message, and Annex F provides information on a standard under development for internal implementation of interception facilities by law enforcement.